

CLAIMS

What is claimed is:

1 1. An apparatus comprising:

2 a first storage to store a platform identifier unique to a platform;

3 a second storage to store an authentication identifier, the authentication
4 identifier being provided by an authentication vendor using the platform
5 identifier, a platform private key, and an authentication private key; and

6 a signature generator to generate a digital signature for data using the
7 platform identifier and the authentication identifier.

1 2. The apparatus of claim 1 wherein the signature generator comprises:

2 a platform-specific transformer to transform the authentication identifier
3 using the platform identifier to output an encrypted platform private key; and

4 a decryptor coupled to the platform-specific transformer to decrypt the
5 encrypted platform private key to generate the platform private key using an
6 authentication public key, the authentication public key being provided by the
7 authentication vendor.

1 3. The apparatus of claim 2 wherein the signature generator further
2 comprises:

1 4. The apparatus of claim 2 wherein the platform-specific transformer
2 comprises:

1 5. The apparatus of claim 2 wherein the platform-specific transformer
2 comprises:

6. The apparatus of claim 2 wherein the authentication identifier is generated by a platform-specific reverse transformer which transforms the encrypted platform private key using the platform identifier, the encrypted platform private key being encrypted from the platform private key using the authentication private key.

20

1 14. An apparatus comprising:

5 a platform-specific reverse transformer to transform the encrypted
6 platform private key to generate an authentication identifier using a platform
7 identifier unique to the platform, the authentication identifier being provided to
8 the platform to generate a digital signature.

3 an Exclusive OR (XOR) device to perform an XOR function on the
4 encrypted platform private key and the platform identifier to generate the
5 authentication identifier.

1 17. The apparatus of claim 14 wherein the platform-specific reverse
2 transformer comprises an encryptor to encrypt the encrypted platform private
3 key using a symmetric encryption/decryption key generated by the platform
4 identifier.

22

6 generating a digital signature for data using the platform identifier and
7 the authentication identifier.

2 transforming the authentication identifier using the platform identifier to
3 output an encrypted platform private key; and

1 20. The method of claim 19 wherein generating the digital signature further
2 comprises:

3 signing the data using the platform private key, the platform private key
4 being transparent to the platform.

1 21. The method of claim 19 wherein transforming the authentication
2 identifier comprises:

1 26. The method of claim 23 wherein transforming the encrypted private key
2 comprises encrypting the encrypted private key using a symmetric
3 encryption/decryption key generated from the platform identifier.

1 36. The computer program product of claim 35 wherein the computer
2 readable program code for generating digital signature comprises:

6 computer readable program code for decrypting the encrypted platform
7 private key to generate the platform private key using an authentication public
8 key provided by the authentication vendor.

3 computer readable program code for signing the data using the platform
4 private key, the platform private key being transparent to the platform.

3 computer readable program code for performing an Exclusive OR (XOR)
4 function on the platform identifier and the authentication identifier.

3 computer-readable program code for decrypting the authentication
4 identifier using a symmetric encryption/decryption key generated from the
5 platform identifier.

1 44. The computer program product of claim 35 wherein the computer
2 readable program code for storing the platform identifier comprises computer
3 readable program code for installing the platform identifier in a protected
4 environment.

7 computer readable program code for transforming the encrypted
8 platform private key to generate an authentication identifier using a platform
9 identifier unique to the platform.

1 49. The computer program product claim of 48 wherein a computer readable
2 program code for transforming the encrypted platform private key comprises:

3 computer readable program code for performing an Exclusive OR (XOR)
4 function on the encrypted platform private key and the platform identifier to
5 generate the authentication identifier.

1 50. The computer program product of claim 49 wherein the platform
2 identifier is a unique, serially uncorrelated bit stream.

1 51. The computer program product of claim 48 wherein the computer
2 readable program code for transforming the encrypted platform private key
3 comprises computer readable program code for encrypting the encrypted
4 platform private key using a symmetric encryption/decryption key generated by
5 the platform identifier.

1 52. A system comprising:

2 a platform having a unique platform identifier (ID); and

3 a digital signature system coupled to the platform to authenticate data,
4 the digital signature system comprising:

5 a first storage to store the platform identifier;

1 53. The system of claim 52 wherein the signature generator comprises:

4 a decryptor coupled to the platform-specific transformer to decrypt the
5 encrypted platform private key to generate the platform private key using an
6 authentication public key, the authentication public key being provided by the
7 authentication vendor.

3 a signer coupled to the decryptor to sign the data using the platform
4 private key, the platform private key being transparent to the platform.

31

1 56. The system of claim 53 wherein the platform-specific transformer
2 comprises:

57. The system of claim 53 wherein the authentication identifier is generated by a platform-specific reverse transformer which transforms the encrypted platform private key and the platform identifier, the encrypted platform private key being encrypted from the platform private key using the authentication private key.

1 59. The system of claim 55 wherein the platform identifier is a unique,
2 serially uncorrelated bit stream.

32

5 an encryptor to encrypt a platform private key using an authentication
6 private key to generate an encrypted platform private key, the platform private
7 key being provided by a platform; and

1 66. The system of claim 65 wherein the platform-specific reverse
2 transformer comprises:

1 67. The system of claim 66 wherein the platform identifier is a unique,
2 serially uncorrelated bit stream.

5 a first storage to store a platform identifier unique to a platform;

34



9

10

1. $2^3 = 8$ $2^4 = 16$ $2^5 = 32$ $2^6 = 64$ $2^7 = 128$ $2^8 = 256$ $2^9 = 512$ $2^{10} = 1024$ $2^{11} = 2048$ $2^{12} = 4096$ $2^{13} = 8192$ $2^{14} = 16384$ $2^{15} = 32768$ $2^{16} = 65536$ $2^{17} = 131072$ $2^{18} = 262144$ $2^{19} = 524288$ $2^{20} = 1048576$ $2^{21} = 2097152$ $2^{22} = 4194304$ $2^{23} = 8388608$ $2^{24} = 16777216$ $2^{25} = 33554432$ $2^{26} = 67108864$ $2^{27} = 134217728$ $2^{28} = 268435456$ $2^{29} = 536870912$ $2^{30} = 1073741824$ $2^{31} = 2147483648$ $2^{32} = 4294967296$ $2^{33} = 8589934592$ $2^{34} = 17179869184$ $2^{35} = 34359738368$ $2^{36} = 68719476736$ $2^{37} = 137438953472$ $2^{38} = 274877906944$ $2^{39} = 549755813888$ $2^{40} = 1099511627776$ $2^{41} = 2199023255552$ $2^{42} = 4398046511104$ $2^{43} = 8796093022208$ $2^{44} = 17592186044416$ $2^{45} = 35184372088832$ $2^{46} = 70368744177664$ $2^{47} = 140737488355328$ $2^{48} = 281474976710656$ $2^{49} = 562949953421312$ $2^{50} = 1125899906842624$ $2^{51} = 2251799813685248$ $2^{52} = 4503599627370496$ $2^{53} = 9007199254740992$ $2^{54} = 18014398509481984$ $2^{55} = 36028797018963968$ $2^{56} = 72057594037927936$ $2^{57} = 144115188075855872$ $2^{58} = 288230376151711744$ $2^{59} = 576460752303423488$ $2^{60} = 1152921504606846976$ $2^{61} = 2305843009213693952$ $2^{62} = 4611686018427387904$ $2^{63} = 9223372036854775808$ $2^{64} = 18446744073709551616$ $2^{65} = 36893488147419103232$ $2^{66} = 73786976294838206464$ $2^{67} = 147573952589676412928$ $2^{68} = 295147905179352825856$ $2^{69} = 590295810358705651712$ $2^{70} = 1180591620717411303424$ $2^{71} = 2361183241434822606848$ $2^{72} = 4722366482869645213696$ $2^{73} = 9444732965739290427392$ $2^{74} = 18889465931478580854784$ $2^{75} = 37778931862957161709568$ $2^{76} = 75557863725914323419136$ $2^{77} = 151115727451828646838272$ $2^{78} = 302231454903657293676544$ $2^{79} = 604462909807314587353088$ $2^{80} = 1208925819614629174706176$ $2^{81} = 2417851639229258349412352$ $2^{82} = 4835703278458516698824704$ $2^{83} = 9671406556917033397649408$ $2^{84} = 19342813113834066795298816$ $2^{85} = 38685626227668133590597632$ $2^{86} = 77371252455336267181195264$ $2^{87} = 154742504910672534362390528$ $2^{88} = 309485009821345068724781056$ $2^{89} = 618970019642690137449562112$ $2^{90} = 1237940039285380274899124224$ $2^{91} = 2475880078570760549798248448$ $2^{92} = 4951760157141521099596496896$ $2^{93} = 9903520314283042199192993792$ $2^{94} = 19807040628566084398385987584$ $2^{95} = 39614081257132168796771975168$ $2^{96} = 79228162514264337593543950336$ $2^{97} = 158456325028528675187087900672$ $2^{98} = 316912650057057350374175801344$ $2^{99} = 633825300114114700748351602688$ $2^{100} = 1267650600228229401496703205376$ $2^{101} = 2535301200456458802993406410752$ $2^{102} = 5070602400912917605986812821504$ $2^{103} = 10141204801825835211973625643008$ $2^{104} = 20282409603651670423947251286016$ $2^{105} = 40564819207303340847894502572032$ $2^{106} = 81129638414606681695789005144064$ $2^{107} = 162259276829213363391578010288128$ $2^{108} = 324518553658426726783156020576256$ $2^{109} = 649037107316853453566312041152512$ $2^{110} = 1298074214633706907132624082305024$ $2^{111} = 2596148429267413814265248164610048$ $2^{112} = 5192296858534827628530496329220096$ $2^{113} = 10384593717069655257060992658440192$ $2^{114} = 20769187434139310514121985316880384$ $2^{115} = 41538374868278621028243970633760768$ $2^{116} = 83076749736557242056487941267521536$ $2^{117} = 166153499473114484112975882535043072$ $2^{118} = 332306998946228968225951765070086144$ $2^{119} = 664613997892457936451903530140172288$ $2^{120} = 1329227995784915872903807060280344576$ $2^{121} = 2658455991569831745807614120560689152$ $2^{122} = 5316911983139663491615228241121378304$ $2^{123} = 10633823966279326983230456482242756608$ $2^{124} = 21267647932558653966460912964485513216$ $2^{125} = 42535295865117307932921825928971026432$ $2^{126} = 85070591730234615865843651857942052864$

[illegible]